

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-244419

(43)Date of publication of application : 29.08.2003

(51)Int.Cl.

H04N 1/387

G06T 1/00

H04N 7/08

H04N 7/081

(21)Application number : 2002-036074

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 13.02.2002

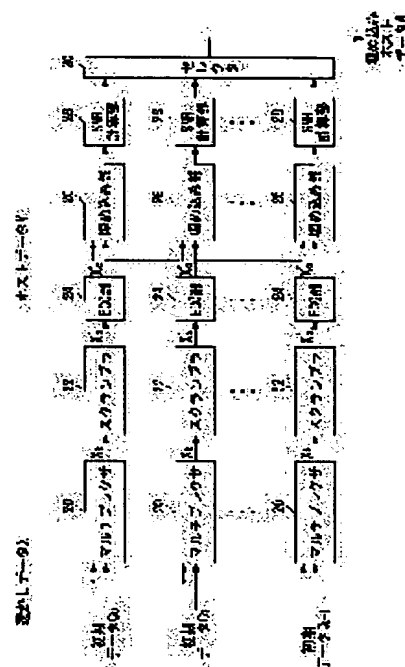
(72)Inventor : KUNIHASHIMA AKIOMI

(54) ELECTRONIC WATERMARK EMBEDDING METHOD, ENCODER AND DECODER CAPABLE OF UTILIZING SUCH METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To solve a problem that it is necessary to strengthen the durability of an electronic watermark since various kinds of operation are applied to the contents data embedded with an electronic watermark.

SOLUTION: A multiplexer 20 produces L kinds of bit sequences by inserting different initial data to the head of watermark data X. A scrambler 22 respectively scrambles the L kinds of bit sequences and produces L kinds of scrambled watermark data X'. An ECC part 24 adds a parity for an error correction to each of data. An embedding part 26 embeds the L kinds of scrambled watermark data X' into host data V and an SNR calculation part 28 evaluates the durability of the watermark data X concerning each of the host data V embedded with the watermark. A selector 30 selects the data of the strongest durability and outputs them as final embedded host data W.



LEGAL STATUS

[Date of request for examination] 24.10.2002

[Date of sending the examiner's decision of rejection] 06.09.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-19447

[Date of requesting appeal against examiner's decision of rejection] 06.10.2005

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-244419

(P2003-244419A)

(43)公開日 平成15年8月29日(2003.8.29)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 5 7
G 0 6 T 1/00	5 0 0	G 0 6 T 1/00	5 0 0 B 5 C 0 6 3
H 0 4 N 7/08		H 0 4 N 7/08	Z 5 C 0 7 6
7/081			

審査請求 有 請求項の数23 O L (全 17 頁)

(21)出願番号 特願2002-36074(P2002-36074)

(22)出願日 平成14年2月13日(2002.2.13)

(71)出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72)発明者 国狭 亜輝臣

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74)代理人 100105924

弁理士 森下 賢樹

Fターム(参考) 5B057 CB19 CE08 CE09 CG07

5C063 AB03 AB07 AC01 AC05 CA11

CA23 DA07 DA13 DB09

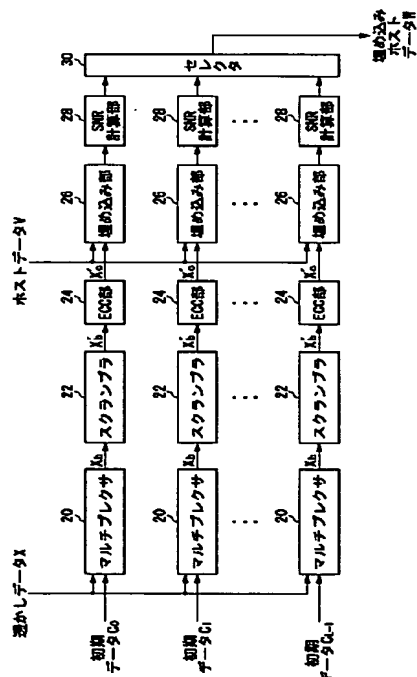
5C076 AA14 BA06

(54)【発明の名称】 電子透かし埋め込み方法およびその方法を利用可能な符号化装置と復号装置

(57)【要約】

【課題】 電子透かしが埋め込まれたコンテンツデータにはさまざまな操作が加えられるため、電子透かしの耐性を強化しなければならない。

【解決手段】 マルチプレクサ20は、透かしデータXの先頭に異なる初期データを挿入してL種類のビット系列を生成する。スクランブラ22はそのL種類のビット系列をそれぞれスクランブルして、L種類のスクランブルされた透かしデータX'を生成し、ECC部24はそれぞれに誤り訂正のためのパリティを付加する。埋め込み部26は、L種類のスクランブルされた透かしデータX'のそれぞれをホストデータVに埋め込み、SNR計算部28は、透かしの埋め込まれたホストデータVのそれぞれについて、透かしデータXの耐性を評価する。セレクタ30は、耐性の最も強いものを選択し、最終的な埋め込みホストデータWとして出力する。



【特許請求の範囲】

【請求項 1】 ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成し、それらの透かしデータの候補がそれぞれ前記ホストデータに埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記透かしデータの埋め込みホストデータを取得することを特徴とする電子透かし埋め込み方法。

【請求項 2】 電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成し、それらの埋め込み位置の候補のそれぞれに前記透かしデータが埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記埋め込み位置に前記透かしデータが埋め込まれた前記ホストデータを取得することを特徴とする電子透かし埋め込み方法。

【請求項 3】 ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成するスクランブル部と、前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含むことを特徴とする符号化装置。

【請求項 4】 電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含むことを特徴とする符号化装置。

【請求項 5】 前記評価部は、前記耐性を、前記ホストデータを前記透かしデータに対するノイズと見なした場合に計算される SN 比により評価することを特徴とする請求項 3 または 4 に記載の符号化装置。

【請求項 6】 前記評価部は、実際に埋め込まれた前記透かしデータと硬判定に基づいて抽出される透かしデータとを比較することにより、前記耐性を評価することを特徴とする請求項 3 または 4 に記載の符号化装置。

【請求項 7】 前記評価部は、前記埋め込みホストデータに対して有用性のある操作を施した上で、前記耐性を評価することを特徴とする請求項 3 から 6 のいずれかに記載の符号化装置。

【請求項 8】 前記評価部は、前記埋め込みホストデー

タを圧縮符号化する際の量子化誤差を考慮して前記耐性を評価することを特徴とする請求項 3 から 6 のいずれかに記載の符号化装置。

【請求項 9】 前記スクランブル部は、スクランブルにより生成される前記透かしデータの候補のデータの一部に、スクランブルを解除するために必要な識別データを含めることを特徴とする請求項 3 に記載の符号化装置。

【請求項 10】 前記スクランブル部によるスクランブルの後、スクランブルを解除するために必要な識別データが秘密鍵として保持されることを特徴とする請求項 3 に記載の符号化装置。

【請求項 11】 前記スクランブル部は、前記識別データに基づく演算により、前記電子透かしデータをスクランブルすることを特徴とする請求項 9 または 10 に記載の符号化装置。

【請求項 12】 前記識別データは前記透かしデータの候補を識別する情報であり、前記スクランブル部は、前記識別データを用いて前記電子透かしデータに畳み込み演算を施すことにより、前記電子透かしデータをスクランブルすることを特徴とする請求項 9 または 10 に記載の符号化装置。

【請求項 13】 前記位置情報生成部は、前記埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、前記複数の埋め込み位置の候補を生成することを特徴とする請求項 4 に記載の符号化装置。

【請求項 14】 前記位置情報生成部による埋め込み位置の候補の生成後、前記識別データが秘密鍵として保持されることを特徴とする請求項 13 に記載の符号化装置。

【請求項 15】 電子透かしの埋め込まれたホストデータからスクランブルされた透かしデータを抽出する抽出部と、前記スクランブルされた透かしデータの識別データをもとに、前記透かしデータに畳み込み演算を施すことにより、前記透かしデータのスクランブルを解除するデスクランブル部とを含むことを特徴とする復号装置。

【請求項 16】 前記デスクランブル部は、前記識別データを前記スクランブルされた透かしデータの一部から取得することを特徴とする請求項 15 に記載の復号装置。

【請求項 17】 前記デスクランブル部は、前記識別データを秘密鍵として取得することを特徴とする請求項 15 に記載の復号装置。

【請求項 18】 電子透かしが埋め込まれたホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、前記複数の埋め込み位置の候補のそれぞれを用いて前記ホストデータに埋め込まれた透かしデータの候補を複数抽出する抽出部と、

前記抽出された複数の透かしデータの候補を想定される透かしデータとの間で照合する照合部と、前記照合部による照合結果に基づいて前記複数の透かしデータの候補の一つを選択して出力する選択部とを含むことを特徴とする復号装置。

【請求項 19】 前記位置情報生成部は、前記埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、前記複数の埋め込み位置の候補を生成することを特徴とする請求項 18 に記載の復号装置。

【請求項 20】 電子透かしが埋め込まれたホストデータの埋め込み位置を識別するための識別データを秘密鍵として取得し、前記秘密鍵に基づいて、前記埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、前記埋め込み位置を特定する位置情報生成部と、前記特定された埋め込み位置を用いて前記ホストデータに埋め込まれた透かしデータを抽出する抽出部とを含むことを特徴とする復号装置。

【請求項 21】 電子透かしデータが埋め込まれたホストデータの構造であって、前記ホストデータに埋め込まれるべき電子透かしデータが所定のスクランブル方式によりスクランブルされた形態で前記ホストデータに埋め込まれており、そのスクランブルされた透かしデータの一部にスクランブルを解除するために必要な当該透かしデータの識別データが含まれることを特徴とするコンピュータにて読み取りおよび利用が可能なデータ構造。

【請求項 22】 ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成する工程と、前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する工程と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項 23】 電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する工程と、前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する工程と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子透かし技術に関し、特に電子透かしの埋め込み方法、およびその方法を利用可能な符号化装置と復号装置に関する。

【0002】

【従来の技術】ここ数年、インターネット利用人口が急増し、インターネット利用の新たなステージともいえるブロードバンド時代に入ろうとしている。ブロードバンド通信では通信帯域が格段に広がるため、音声、静止画、動画などデータ量の大きいコンテンツの配信も気軽にできるようになる。このようなデジタルコンテンツの流通が盛になると、コンテンツの著作権の保護がより一層求められることになる。

【0003】ネットワーク上に流通するコンテンツのデータは他人に容易にコピーされ、著作権に対する保護が十分ではないのが現状である。そこで著作権を保護するために、コンテンツの作成者や利用者の情報を電子透かしとしてコンテンツデータに埋め込む技術が開発されている。この電子透かし技術を用いることにより、ネットワーク上で流通するコンテンツデータから電子透かしを抽出して、不正利用を検出したり、不正コピーの流通経路を追跡することが可能となる。

【0004】

【発明が解決しようとする課題】電子透かしは、不正利用者による改ざんを防止するために、利用者には分からないようにコンテンツデータに埋め込まれる。しかしコンテンツデータは、流通過程や利用過程で、圧縮符号化や各種フィルタリングなどの信号処理が加えられたり、ユーザにより加工されたり、あるいは透かし情報が改ざんされるなど、さまざまな操作を受けることがあり、その過程で埋め込まれた電子透かしデータの一部が変更されたり、消失する可能性がある。したがって電子透かしはこういった操作に対する耐性が要求される。

【0005】電子透かしの耐性を高めるためにさまざまな電子透かしの埋め込み技術が開発されている。たとえば、特開 2000-13587 号公報は、電子透かし情報を埋め込む処理の自由度を維持しつつ、耐性の強い電子透かしの埋め込みを可能とする埋め込み方法が開示されている。このような電子透かし技術は、人間の視覚特性に合わせて、画像のエッジ部分やテキスト領域の中でも変化の大きな部分など高周波成分に電子透かしを埋め込む方法であり、個々のコンテンツデータの内容に強く依存し、透かし埋め込み後のコンテンツデータに対するさまざまな操作に対して耐性を強化するには、汎用性や柔軟性の面で限界がある。

【0006】本発明はこうした状況に鑑みてなされたもので、その目的は、耐性の強い電子透かしを埋め込み、電子透かしの検出誤差を低減することの可能な技術の提供にある。

【0007】

10

20

30

40

50

【課題を解決するための手段】本発明のある態様は電子透かし埋め込み方法に関する。この方法は、ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成し、それらの透かしデータの候補がそれぞれ前記ホストデータに埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記透かしデータの埋め込みホストデータを取得する。この方法によれば、ホストデータに応じて、透かしデータを耐性の強いデータ系列に変換した後

に埋め込むことができ、電子透かしの検出誤差を低減することができる。

【0008】ホストデータは、電子透かしを埋め込む対象となるオリジナルデータであり、たとえば静止画、動画、音声などのデータである。埋め込まれる電子透かしには、オリジナルデータの識別情報、作成者情報、利用者情報などが含まれる。その他、認証を目的として、ホストデータのダイジェストデータ、すなわちホストデータの特徴を端的に表したデータを電子透かしとして埋め込むことも可能である。電子透かしの耐性とは、電子透かしの埋め込まれたホストデータが改変されるなどの攻撃を受けた場合や、埋め込みホストデータに圧縮符号化やフィルタリングなどの信号処理が施された場合など、埋め込みホストデータに対して何らかの操作が加えられた場合に電子透かしデータがもつ頑強性をいう。

【0009】電子透かしを埋め込む側では、電子透かしデータをスクランブルする際、元の電子透かしデータを複数の透かしデータの候補に対応づける1対多の写像が用いられる。電子透かしを抽出する側では、逆写像を行って、スクランブルされた透かしデータから元の電子透かしデータを得る。そのため電子透かしを抽出する側では、元の電子透かしデータと複数の透かしデータの候補の対応テーブルが利用されてもよい。また、電子透かしを埋め込む側で、元の電子透かしデータから所定の初期値のもとで複数の透かしデータの候補を生成するスクランブル関数が利用されてもよい。この場合、電子透かしを抽出する側では、スクランブルに利用された初期値とスクランブル関数にもとづいて、抽出された電子透かしの逆スクランブルが行われる。

【0010】本発明の別の態様も電子透かし埋め込み方法に関する。この方法は、電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成し、それらの埋め込み位置の候補のそれぞれに前記透かしデータが埋め込まれた場合における当該電子透かしの耐性を評価し、その評価が良好である前記埋め込み位置に前記透かしデータが埋め込まれた前記ホストデータを取得する。埋め込み位置の候補は、初期埋め込み位置を所定の初期値のもとでスクランブル関数によりスクランブルすることで生成してもよい。この方法によれば、ホストデータの応じて、耐性が強い埋め込み位置を検出して、電子透かしを埋め込むことができる。

【0011】本発明のさらに別の態様は符号化装置に関する。この装置は、ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成するスクランブル部と、前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含む。

【0012】本発明のさらに別の態様も符号化装置に関する。この装置は、電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、前記ホストデータの埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する埋め込み部と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する評価部と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択して出力する選択部とを含む。

【0013】前記スクランブル部は、前記識別データに基づく演算により、前記電子透かしデータをスクランブルしてもよい。この演算はスクランブル多項式その他の変換式により透かしデータを変換する演算であってもよい。前記スクランブル部は、前記透かしデータの候補を識別するための識別データを用いて前記電子透かしデータに畳み込み演算を施すことにより、前記電子透かしデータをスクランブルしてもよい。この畳み込み演算により、多様性に富んだ透かしデータの候補を生成することができる。埋め込み位置の候補を生成する際にも、このスクランブル方式が用いられてもよい。また埋め込み位置の候補を識別するための識別データとランダムな埋め込み位置とを対応づけたテーブルを参照することにより、複数の埋め込み位置の候補を生成してもよい。

【0014】前記スクランブル部は、スクランブルにより生成される前記透かしデータの候補のデータの一部に、スクランブルを解除するために必要な識別データを含めてもよい。前記スクランブル部によるスクランブルの後、スクランブルを解除するために必要な識別データが秘密鍵として保持されてもよい。この識別データはスクランブル方式を特定する情報、たとえばスクランブルの種類、スクランブルの変換式または逆変換式を識別する情報であってもよい。またこの識別データはスクランブルを解除するために必要な初期データを含んでもよい。復号側でスクランブルされた電子透かしを抽出した際、この識別データをもとにしてスクランブルを解除して、元の電子透かしデータを得ることができる。

【0015】上記のいずれの符号化装置においても、前記評価部は、前記耐性を、前記ホストデータを前記透かしデータに対するノイズと見なした場合に計算されるS

N比により評価してもよい。特にターボ符号化などの軟入力誤り訂正符号の場合には、SN比に基づいた評価基準で候補を選択することにより、ビット誤り率(BER)を低減することができる。また、前記評価部は、実際に埋め込まれた前記透かしデータと硬判定に基づいて抽出される透かしデータとを比較することにより、前記耐性を評価してもよい。この比較のために、硬判定により抽出される透かしデータと実際に埋め込まれた透かしデータとの間のハミング距離もしくはユークリッド距離を評価してもよい。この場合、距離が大きいほど、誤差が大きいと、強度は低いと判断される。この評価基準により、正しく硬判定復号されるビット数が最も多い透かしデータの候補が選択される。特に硬入力に基づいた誤り訂正符号を用いる場合は、このような硬判定結果との比較評価基準で候補を選択することにより、ビット誤り率を低く抑えることができる。

【0016】前記評価部は、前記埋め込みホストデータに対して有用性のある操作を施した上で、前記耐性を評価してもよい。有用性のある操作とは、たとえば圧縮符号化や各種フィルタリングなどの信号処理、スケーリングや回転などの幾何学的変換などである。前記評価部は、前記埋め込みホストデータを圧縮符号化する際の量子化誤差を考慮して前記耐性を評価してもよい。前記耐性をSN比で評価する場合、埋め込みホストデータに有用性のある操作を施した後に抽出される透かしデータと実際に埋め込まれた透かしデータとの間の分散を評価してもよい。

【0017】本発明のさらに別の態様は復号装置に関する。この装置は、電子透かしの埋め込まれたホストデータからスクランブルされた透かしデータを抽出する抽出部と、前記スクランブルされた透かしデータの識別データをもとに、前記透かしデータに畳み込み演算を施すことにより、前記透かしデータのスクランブルを解除するデスクランブル部とを含む。前記デスクランブル部は、前記識別データを前記スクランブルされた透かしデータの一部から取得してもよい。

【0018】本発明のさらに別の態様は復号装置に関する。この装置は、電子透かしが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、前記複数の埋め込み位置の候補のそれぞれを用いて前記ホストデータに埋め込まれた透かしデータの候補を複数抽出する抽出部と、前記抽出された複数の透かしデータの候補を、想定される透かしデータとの間で照合する照合部と、前記照合部による照合結果に基づいて前記複数の透かしデータの候補の一つを選択して出力する選択部とを含む。

【0019】本発明のさらに別の態様はコンピュータにて読み取りおよび利用が可能なデータ構造に関する。このデータ構造は、電子透かしデータが埋め込まれたホストデータの構造であり、ホストデータに埋め込まれるべ

き電子透かしデータが所定のスクランブル方式によりスクランブルされた形態で前記ホストデータに埋め込まれており、そのスクランブルされた透かしデータの一部にスクランブルを解除するために必要な当該透かしデータの識別データが含まれる。

【0020】本発明のさらに別の態様はコンピュータプログラムに関する。このプログラムは、ホストデータに埋め込まれるべき電子透かしデータをスクランブルして複数の透かしデータの候補を生成する工程と、前記複数の透かしデータの候補をそれぞれ前記ホストデータに埋め込み、複数の埋め込みホストデータの候補を生成する工程と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させる。

【0021】本発明のさらに別の態様もコンピュータプログラムに関する。このプログラムは、電子透かしデータが埋め込まれるホストデータの埋め込み位置の候補を複数生成する工程と、前記ホストデータの前記複数の埋め込み位置の候補のそれぞれに前記透かしデータを埋め込み、複数の埋め込みホストデータの候補を生成する工程と、前記複数の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する工程と、前記耐性の評価値に基づいて前記複数の埋め込みホストデータの候補の一つを選択する工程とをコンピュータに実行させる。

【0022】なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【0023】

【発明の実施の形態】実施の形態1

図1は、実施の形態1に係る符号化装置10の構成を示す。この構成は、ハードウェア的には、任意のコンピュータのCPU、メモリ、その他のLSIで実現でき、ソフトウェア的にはメモリにロードされた電子透かし埋め込み機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組み合わせによっていろいろな形で実現できることは、当業者には理解されるところである。

【0024】符号化装置10は、ホストデータVに透かし情報Iを埋め込む処理を行い、埋め込みホストデータWを出力する。ホストデータVは、たとえば音声、静止画、動画などのデータである。透かし情報Iは、そのホストデータVの識別情報、作成者情報、利用者情報など著作権に関する情報、ホストデータVの改ざん検出を行う認証情報、タイムスタンプなどである。

10

20

30

40

50

【0025】暗号化部12は、ホストデータVに埋め込むべき透かし情報Iを秘密鍵Kにより暗号化し、透かしデータXを出力する。暗号化の関数を f 。とすると、この処理は変換式 $X=f$ 。(I, K)で表される。透かし情報の暗号化を行わない場合には、暗号化部12の構成は省略してもよい。

【0026】変更部14は、透かしデータXとホストデータVを用いて、透かしデータXをスクランブルし、スクランブルされた透かしデータX'を出力する。スクランブルの関数を f_2 とすると、この処理は変換式 $X' = f_2(X, V)$ で表される。

【0027】埋め込み部16は、秘密鍵Kを用いて、スクランブルされた透かしデータX'をホストデータVに埋め込み、埋め込みホストデータWを出力する。埋め込みの関数を f_1 とすると、この処理は変換式 $W = f_1(V, X', K)$ で表される。秘密鍵Kに依存しない埋め込み方式の場合は、 $W = f_1(V, X')$ となる。

【0028】変更部14と埋め込み部16は協同して、複数のスクランブルされた透かしデータX'を生成し、それぞれをホストデータVに埋め込み、複数の埋め込みホストデータWの候補を生成し、それらの候補の一つを選択する機能をもつ。

【0029】図2は変更部14と埋め込み部16の機能構成図である。L個のマルチプレクサ20は、透かしデータXの先頭にそれぞれ初期データ $C_0 \sim C_{L-1}$ を挿入したL種類のビット系列X。を生成する。L個のスクランブラ22はL種類のビット系列をそれぞれスクランブルして、L種類のスクランブルされた透かしデータX'。を生成する。L個のECC(Error Correction Code)部24はL種類のスクランブルされた透かしデータX'。のそれぞれに誤り訂正のためのパリティを付加した透かしデータX'。を生成する。ECC部24は、透かしビットの検出率を向上させるためのオプションであって、アプリケーションによっては必要ない場合もあり、この構成を省略してもよい。

【0030】L個の埋め込み部26は、L種類のスクランブルされた透かしデータX'。のそれぞれをホストデータVに埋め込み、L種類の埋め込みホストデータWの候補を生成する。L個のSNR計算部28は、L種類の埋め込みホストデータWの候補のそれぞれについて、透かしデータXの耐性を評価する。セクタ30は、耐性の評価値が最良である埋め込みホストデータWの候補を選択し、それを最終的な埋め込みホストデータWとして出力する。

【0031】図3は、実施の形態1に係る復号装置40の構成を示す。符号化装置10により電子透かしが埋め込まれた埋め込みホストデータWは、ネットワーク上で流通し、コンピュータにおいて利用される。その過程で埋め込みホストデータWは圧縮符号化や改ざんなどの操作を受ける。画像データであれば、JPEG圧縮、フ

ルタリング、量子化、色補正などの信号処理や、スケーリング、クロッピング、回転、並行移動等の幾何学的な変換など有用性のある操作が施されたり、電子透かしを除去したり改変するなどの不正な攻撃が加えられたりする。そのような操作による変形を埋め込みホストデータWに対するノイズNとみなし、ノイズNが付加した埋め込みホストデータWを埋め込みホスト信号W'($=W+N$)とする。復号装置40は、埋め込みホスト信号W'から埋め込まれた透かしデータXを抽出する処理を行う。

【0032】抽出部42は、秘密鍵Kを用いて、埋め込みホスト信号W'に埋め込まれた透かしデータX'。を抽出する。ECC復号部44はこの透かしデータX'。に付加されているパリティビットを用いて誤り訂正を行い、透かしデータX'。を生成する。デスクランブラ46は秘密鍵Kを用いて、誤り訂正後の透かしデータX'。のスクランブルを解除し、透かしデータX。を出力する。図示しないが、この透かしデータX。はさらに、秘密鍵Kにより復号されて元の透かし情報Iが得られる。

【0033】以上の構成の符号化装置10および復号装置40による電子透かしの埋め込みと抽出の手順を説明する。図8は、符号化装置10による電子透かしの埋め込み手順を説明するフローチャートである。フローチャートの説明にあたり、図4から図7を適宜参照する。マルチプレクサ20は、暗号化部12により暗号化された透かしデータXの先頭にL種類の初期データを挿入してL個の符号系列を生成し(S10)、スクランブラ22は、それらの符号系列をスクランブルしてL種類のスクランブルされた透かしデータX'を生成する(S12)。

【0034】図4は、透かしデータXとL種類のスクランブルされた透かしデータX'との関係を示す。nビットの透かしデータXの先頭に、rビットの冗長語を識別データID[0]~ID[L-1]として付加し、L種類の透かしデータの候補を作成する。最大 2^r 種類の候補が作成される。これらの候補に含まれる透かしデータXのビット列はこれから述べるスクランブル方式により、スクランブルされる。

【0035】スクランブル方式の一例として、伝送や磁気記録におけるデジタル変調の際に利用されるGS(Guided Scramble)方式を採用する。GS方式は、ある一定のデータブロック長からなる情報系列に対して、L種類の符号系列を生成し、これらを次に送信する符号系列の候補として扱う。これらの候補の中から、伝送媒体の性質に合わせて最適なものを選択して最終的な符号系列とする。このGS方式により、多様性に富んだ符号系列の候補を簡単な方法で生成することができる。

【0036】符号化装置10におけるマルチプレクサ20とスクランブラ22がGS符号化器として機能する。GS符号化器は、nビットからなる情報系列D(x)の

直前にL種類のrビットの冗長語 c_i ($i=0, \dots, L-1$)を付加し、L種類の符号系列 $c_i x^n + D(x)$ を生成する。この符号系列の符号長は $(n+r)$ ビットとなる。このようにして冗長語が付加された符号*

$$T_i(x) = Q_s(x) [(c_i x^n + D(x)) x^n] \quad (1)$$

ただし、 Q_s 、 $[b]$ は b を a で除算した商を示す。商集合 $\{T_0(x), \dots, T_{L-1}(x)\}$ がスクランブル後の符号系列の候補である。これらの候補の各々について、その符号系列が実際に用いられた際の性能を評価し、その評価値が最良であるものを最終的な符号系列として選択する。

【0038】復調時には、復号装置40におけるデスクランブラ46がGS復号器として機能し、符号系列に $S(x)$ を乗算し、下位Nビットと上位rビットの変換情報を捨てることにより、元の情報系列 $D(x)$ が得られる。

【0039】ここでスクランブル多項式 $S(x)$ として、 $S(x) = x^r + 1$ を用いた場合を説明する。 $n \bmod r = 0$ の場合、(1)式は次式に示す畳み込み演算で表現可能である。

$$\begin{aligned} t_j &= d_j (+) c_i \quad (j=0) \\ t_j &= d_j (+) t_{j-1} \quad (j=1, \dots, n/r-1) \end{aligned}$$

ただし、 $i=0, \dots, L-1$ であり、 d_j は元の情報系列 $D(x)$ をrビットずつ区切ったビット列、 t_j は変換後の符号系列 $T_i(x)$ の先頭のrビットの冗長語 c_i 以降をrビットずつ区切ったビット列である。また(+)は排他的論理和(EX-OR)演算を示す。

【0041】図5はこの符号化時の畳み込み演算を説明する図である。たとえば、 $n=6$ 、 $r=2$ の場合を考える。元の情報系列 $D(x) = (1, 0, 1, 0, 0, 1)$ に対して、冗長語 $c_0 = (0, 0)$ を付加して、変換後の符号系列 $T_0(x)$ を生成する。上記の符号化時の畳み込み演算により、 $t_0 = d_0 (+) c_0 = (1, 0) (+) (0, 0) = (1, 0)$ 、 $t_1 = d_1 (+) t_0 = (1, 0) (+) (1, 0) = (0, 0)$ 、 $t_2 = d_2 (+) t_1 = (0, 1) (+) (0, 0) = (0, 1)$ となり、変換後の符号系列 $T_0 = (0, 0, 1, 0, 0, 0, 0, 1)$ が得られる。ここで変換後の符号系列 T_0 の先頭の2ビットは冗長語 c_0 であることに注意する。

※ 【0048】

$$\begin{aligned} x^0 &= \{-1, \dots, -1, -1, x^0_0, x^0_1, \dots, x^0_{n-1}\} \\ x^1 &= \{-1, \dots, -1, 1, x^1_0, x^1_1, \dots, x^1_{n-1}\} \\ &\dots \\ x^{L-1} &= \{1, \dots, 1, 1, x^{L-1}_0, x^{L-1}_1, \dots, x^{L-1}_{n-1}\} \end{aligned}$$

【0049】nビットの透かしデータの埋め込み対象として選択されたホストデータVのサンプルの集合のペア (V^+, V^-) を次のように定義する。サンプルの集合 V^+ 、 V^- は次のようにそれぞれn個の要素をもつ。な

* 系列に対して、次式のようにN次元のスクランブル多項式 $S(x)$ で除算することにより商 $T_i(x)$ を求める。

【0037】

※ 【0042】同様にして、冗長語 $c_1 = (0, 1)$ 、 $c_2 = (1, 0)$ 、 $c_3 = (1, 1)$ に対して、それぞれ変換後の符号系列 $T_1 = (0, 1, 1, 1, 0, 1, 0, 0)$ 、 $T_2 = (1, 0, 0, 0, 1, 0, 1, 1)$ 、 $T_3 = (1, 1, 0, 1, 1, 1, 1, 0)$ が得られる。

【0043】復号時は次式のように畳み込み演算を行うことにより、元の情報系列 $D(x)$ が得られる。

$$\begin{aligned} d_j &= t_j (+) c_i \quad (j=0) \\ d_j &= t_j (+) t_{j-1} \quad (j=1, \dots, n/r-1) \end{aligned}$$

【0045】図6はこの復号時の畳み込み演算を説明する図である。前述の例において、変換後の符号化系列 $T_0 = (0, 0, 1, 0, 0, 0, 0, 1)$ が与えられると、先頭の2ビットから冗長語 $c_0 = (0, 0)$ が得られ、上記の復号時の畳み込み演算により、 $d_0 = t_0 (+) c_0 = (1, 0) (+) (0, 0) = (1, 0)$ 、 $d_1 = t_1 (+) t_0 = (0, 0) (+) (1, 0) = (1, 0)$ 、 $d_2 = t_2 (+) t_1 = (0, 1) (+) (0, 0) = (0, 1)$ となり、元の情報系列 $D(x) = (1, 0, 1, 0, 0, 1)$ が得られる。他の変換後の符号化系列 T_1 、 T_2 、 T_3 についてもこの畳み込み演算により、元の情報系列 $D(x)$ が得られる。

【0046】再び図8を参照する。スクランブラ22によって生成されたL種類のスクランブルされた透かしデータ X' は、ECC部24により誤り訂正のためのパリティを付加された後に、埋め込み部26によりホストデータVに埋め込まれる(S14)。

【0047】図7(a)、(b)は、スクランブルされた透かしデータ X' の埋め込み方法を説明する図である。L種類のスクランブルされた透かしデータ X' を x^0, x^1, \dots, x^{L-1} とする。各透かしデータの候補のビット系列は、次式のように表される。先頭のrビットは識別データである。また、スクランブル処理後のビット0は、-1に置き換えて、以下の処理を行う。

※ 【0048】

$$\begin{aligned} x^0 &= \{-1, \dots, -1, -1, x^0_0, x^0_1, \dots, x^0_{n-1}\} \\ x^1 &= \{-1, \dots, -1, 1, x^1_0, x^1_1, \dots, x^1_{n-1}\} \\ &\dots \\ x^{L-1} &= \{1, \dots, 1, 1, x^{L-1}_0, x^{L-1}_1, \dots, x^{L-1}_{n-1}\} \end{aligned}$$

お、ホストデータVは、空間軸上のサンプル、時間軸上のサンプル、周波数軸上のサンプル、たとえばDCT変換、FFT変換、DWT変換などの処理後のサンプルなどにより表現される。

【0050】

$$V^+ = \{v^+_{i,0}, v^+_{i,1}, \dots, v^+_{i,n-1}\}$$

$$V^- = \{v^-_{i,0}, v^-_{i,1}, \dots, v^-_{i,n-1}\}$$

ここでサンプルの集合 V^+ , V^- の要素である各サブセ

$$v^+_{i,j} = \{v^+_{i,j,0}, v^+_{i,j,1}, \dots, v^+_{i,j,m-1}\}$$

$$v^-_{i,j} = \{v^-_{i,j,0}, v^-_{i,j,1}, \dots, v^-_{i,j,m-1}\}$$

【0052】透かしデータの候補 x^k ($k=0, \dots, L-1$) をサンプルの集合のペア (V^+ , V^-) に次のように埋め込み、 L 種類の埋め込みホストデータの候補 W^k を生成する。

【0053】

$$w^+_{i,j} = v^+_{i,j} + \alpha^+_{i,j} \cdot x^k_{i,j}$$

$$w^-_{i,j} = v^-_{i,j} - \alpha^-_{i,j} \cdot x^k_{i,j}$$

ここで $\alpha^+_{i,j}$ および $\alpha^-_{i,j}$ は人間の視覚モデルにもとづいて知覚されるノイズを減少するためのスケールパラメータであり、いずれも正の値である。あるいは、 $\alpha^+_{i,j}$ および $\alpha^-_{i,j}$ は、ある確率分布、たとえばガウシアン分布、一様分布などに従うように、秘密鍵 K によって生成される正の値であってもよい。この場合、透かしの埋め込み強度は減少するが、埋め込まれた透かしの秘匿性は向上する。このようにして、 k 番目の透かしデータの候補の各ビット $x^k_{i,j}$ は各サブセット $v^+_{i,j}$, $v^-_{i,j}$ のそれぞれ m 個のサンプルに重複して埋め込まれる。重複の数 m が大きいほど、透かしビットが失われる可能性が低くなり、検出誤差が小さくなる一方で、ホストデータに埋め込むことができる透かしのビット数が減少する。 $\alpha^+_{i,j}$ および $\alpha^-_{i,j}$ は、視覚上の劣化を検知できないように各ピクセル毎に設定される値であり、原理的には、埋め込むピクセル数 m を増やしても、人間の視覚上、画質の劣化は検知されない。しかし、1 ビットを埋め込むのに費やすピクセル数が増加するということは、埋め込み領域には制限があるため、埋め込むことができるビット数が減少することを意味し、したがって埋め込み率の低下を招くこととなる。 ※

$$W'^+ = \{w'^+_{i,0}, w'^+_{i,1}, \dots, w'^+_{i,n-1}\}$$

$$W'^- = \{w'^-_{i,0}, w'^-_{i,1}, \dots, w'^-_{i,n-1}\}$$

ここで埋め込みホスト信号の集合 W'^+ , W'^- の要素である各サブセット $w'^+_{i,j}$, $w'^-_{i,j}$ は、電子透かし

$$w'^+_{i,j} = \{w'^+_{i,j,0}, w'^+_{i,j,1}, \dots, w'^+_{i,j,m-1}\}$$

$$w'^-_{i,j} = \{w'^-_{i,j,0}, w'^-_{i,j,1}, \dots, w'^-_{i,j,m-1}\}$$

【0058】透かしビット $x^k_{i,j}$ を検出するために、次

$$\begin{aligned} z_i &= \sum_{j=0}^{m-1} (w'^+_{i,j} - w'^-_{i,j}) \\ &= \sum_{j=0}^{m-1} [(w^+_{i,j} + \alpha^+_{i,j} \cdot x^k_{i,j}) - (w^-_{i,j} + \alpha^-_{i,j} \cdot x^k_{i,j})] \\ &= \sum_{j=0}^{m-1} [(v^+_{i,j} - v^-_{i,j}) + (\alpha^+_{i,j} + \alpha^-_{i,j}) \cdot x^k_{i,j} + (n^+_{i,j} - n^-_{i,j})] \end{aligned}$$

ここで $\sum_{j=0}^{m-1} (v^+_{i,j} - v^-_{i,j})$ は m が十分に大きいとき、一般にガウス分布に従い、0 に近づく。またノイズの項 $\sum_{j=0}^{m-1} (n^+_{i,j} - n^-_{i,j})$ についても同様に 0 に近づく。したがって、

※ ユット $v^+_{i,j}$, $v^-_{i,j}$ は、次のようにホストデータ V の m 個のサンプルデータからなる。

【0051】

※ 【0054】各サブセット $v^+_{i,j}$, $v^-_{i,j}$ は、一例としてホストデータ V を離散コサイン変換 (Discrete Cosine Transform) したときに得られる DCT ブロックであり、透かしビットの埋め込み対象として選ばれる m 個のサンプルデータは、DCT ブロックに含まれる m 個の DCT 係数である。図 7 (a)、(b) は、 8×8 の DCT ブロックのペア $v^+_{i,j}$, $v^-_{i,j}$ のそれぞれ m 個の DCT 係数に透かしデータ $x^k_{i,j}$ が埋め込まれる様子を示している。ブロックペア $v^+_{i,j}$, $v^-_{i,j}$ および m 個の DCT 係数は、秘密鍵 K に基づいて選択される。

【0055】図 8 に戻り、SNR 計算部 28 は、 L 種類の埋め込みホストデータの候補 W^k に対して透かしデータ x^k の耐性、すなわち埋め込み強度を評価し (S16)、セレクト部 30 は埋め込み強度が最大となる埋め込みホストデータの候補 W^k を最終的な埋め込みホストデータ W として選択する (S18)。

【0056】埋め込み強度の評価式を与える前に、埋め込みホストデータ W に対して信号処理や画像処理などにより変形が加えられた場合に、透かしデータ X' がどのように検出されるかを検討する。埋め込みホストデータ W に加えられる変形をノイズ N として扱い、ノイズ N が加わった埋め込みホストデータ W を埋め込みホスト信号 W' と呼ぶ。この埋め込みホスト信号 W' から透かしデータ X' を抽出する方法を説明する。埋め込みホスト信号の集合のペア (W'^+ , W'^-) を次のように定義する。埋め込みホスト信号の集合 W'^+ , W'^- は次のようにそれぞれ n 個の要素をもつ。

【0057】

★の埋め込み位置に対応して、次のように埋め込みホスト信号 W' の m 個のサンプルデータからなる。

☆の判定値 z_i を計算する。

z_i は $\sum_{j=0}^{m-1} [(\alpha^+_{i,j} + \alpha^-_{i,j}) \cdot x^k_{i,j}]$ の値で近似できる。 $(\alpha^+_{i,j} + \alpha^-_{i,j})$ は正であるから、透かしビット $x^k_{i,j}$ が 1 ならば z_i は正であり、透かしビット $x^k_{i,j}$ が -1 なら

ば z_i は負である。したがって z_i の正負により透かしビット x^k_i の値を判定することができる。

【0059】埋め込み強度の評価は、ホストデータ V を透かしデータ X に対するノイズとみなして、埋め込まれた透かしデータ x^k に対して検出される透かしデータの*

$$K = \arg \max_k \left(P_k / (2 \sigma_k^2) \right) \\ P_k = \sum_{i=0}^{n-1} \left| \sum_{j=0}^{m-1} (w^{+k}_{i,j} - w^{-k}_{i,j}) \right|^2 / n \\ \sigma_k^2 = \sum_{i=0}^{n-1} \left| \sum_{j=0}^{m-1} (w^{+k}_{i,j} - w^{-k}_{i,j}) - P_k^{1/2} \cdot x^k_i \right|^2 / n$$

【0061】透かしビット x^k_i が $\{1, -1\}$ のいずれであるかを判定するための前述の判定値 z_i は、埋め込みホストデータ W にノイズが付加される前の状態では、 $z_i = \sum_{j=0}^{m-1} (w^{+k}_{i,j} - w^{-k}_{i,j})$ で与えられることを考慮すると、分散 σ_k^2 は、判定値 z_i により検出される透かしビットと実際に埋め込まれた透かしビット x^k_i の差を $i=0, \dots, n-1$ について評価して合計したものであると言える。一方、 P_k は判定値 z_i の $i=0, \dots, n-1$ についての自乗和である。したがって、埋め込まれた透かしデータ x^k と抽出される透かしデータとの間のハミング距離もしくはユークリッド距離が小さく、透かしビットを検出するための判定値の絶対値が大きいほど、 $P_k / (2 \sigma_k^2)$ の値は大きくなる。言い換えれば、 $P_k / (2 \sigma_k^2)$ が最大となる候補を選択することは、透かしビットの検出誤差が最小である候補を選択することを意味する。

【0062】判定値 z_i について、 $v^{+}_{i,j} > v^{+}_{i,j}$ かつ $x^k_i = 1$ ならば $z_i > 0$ となり、 $v^{+}_{i,j} > v^{+}_{i,j}$ かつ $x^k_i = -1$ ならば $z_i < 0$ となる。したがって前述の評価により最適な透かしデータ x^k の候補を選択することは、判定値 z_i による透かしビット x^k_i の検出性能を向上させるために、 $v^{+}_{i,j} > v^{+}_{i,j}$ ならば $x^k_i = 1$ となり、 $v^{+}_{i,j} < v^{+}_{i,j}$ ならば $x^k_i = -1$ となるように、元の透かしビット x_i を x^k_i に変更することを意味する。これがGS方式のガイディングルールであり、これにより判定値 z_i のレスポンスが改善する。

$$z_i = \sum_{j=0}^{m-1} (w^{+}_{i,j} - w^{-}_{i,j}) \\ = \sum_{j=0}^{m-1} [(w^{+}_{i,j} + n^{+}_{i,j}) - (w^{-}_{i,j} + n^{-}_{i,j})] \\ = \sum_{j=0}^{m-1} [(v^{+}_{i,j} - v^{-}_{i,j}) + (\alpha^{+}_{i,j} + \alpha^{-}_{i,j}) \cdot x^k_i + (n^{+}_{i,j} - n^{-}_{i,j})]$$

【0065】抽出された透かしデータ X' はさらにECC復号部44により誤り訂正がなされ、デスクランブラ46によりスクランブルを解除され、元の透かしデータ X が得られる。

【0066】以上述べたように、実施の形態によれば、GS方式を用いて、電子透かしを埋め込む画像や音声などのメディアデータが与えられると、透かしビット系列をそのメディアデータに埋め込みやすいビット系列に変換した上で埋め込むことができる。したがって信号処理、幾何変換、圧縮、データの改ざんなどに対する電子透かしの耐性を強化することができ、透かしの検出精度が大幅に改善する。

【0067】上記の実施の形態では、図2で示したように、L種類の透かしデータの候補を生成するために、L個のマルチプレクサ20、スクランブラ22、ECC部24、埋め込み部26、およびSNR計算部28が並列

*分散を計算することにより行われる。分散が小さいほど、耐性強いと考えることができる。埋め込みホストデータの候補のペア (W^{+k}, W^{-k}) に対して次式により分散を評価して、最適な候補 K を選択する。

【0060】

※ $v^{+}_{i,j} < v^{+}_{i,j}$ かつ $x^k_i = -1$ ならば $z_i < 0$ となる。したがって前述の評価により最適な透かしデータ x^k の候補を選択することは、判定値 z_i による透かしビット x^k_i の検出性能を向上させるために、 $v^{+}_{i,j} > v^{+}_{i,j}$ ならば $x^k_i = 1$ となり、 $v^{+}_{i,j} < v^{+}_{i,j}$ ならば $x^k_i = -1$ となるように、元の透かしビット x_i を x^k_i に変更することを意味する。これがGS方式のガイディングルールであり、これにより判定値 z_i のレスポンスが改善する。

20 【0063】復号装置40の抽出部42は、ノイズの付加された埋め込みホスト信号 W' を受け取ると、ECC復号部44が硬入力の復号器で構成される場合には、判定値 z_i を次のように計算し、判定値 z_i の正負で、透かしビット x' が $\{-1, 1\}$ のいずれであるかを判定し、透かしデータ X' を得る。また、ECC復号部44が軟入力の復号器で構成される場合には、判定値 z_i を $\{-1, 1\}$ に硬判定することなく、そのまま、ECC復号部44に送る。

【0064】

に設けられたが、これらの部材を単一構成にして、L種類の透かしデータの候補を逐次的に生成、評価して最適な候補を選択してもよい。

【0068】図9は、そのような逐次型の電子透かしの埋め込み手順を説明するフローチャートである。変数 i を1に初期化する (S20)。マルチプレクサ20は、暗号化部12により暗号化された透かしデータ X の先頭に i 番目の初期データを挿入して符号系列を生成し (S22)、スクランブラ22は、その符号系列をスクランブルして、 i 番目のスクランブルされた透かしデータ X' を生成する (S24)。スクランブラ22によって生成された i 番目のスクランブルされた透かしデータ X' は、必要に応じてECC部24により誤り訂正のためのパリティを付加された後に、埋め込み部26によりホストデータ V に埋め込まれる (S26)。SNR計算部28は、 i 番目の埋め込みホストデータの候補 W^i に

対して透かしデータ x^i の耐性、すなわち埋め込み強度 S_i を評価する (S28)。セレクト 30 は、埋め込み強度 S_i が最低の評価値を保証する基準値 T より大きいかどうかを判定する (S30)。もし埋め込み強度 S_i が基準値 T より大きければ (S30 の Y)、変数 K に現在の変数 i の値を代入し (S32)、 K 番目の埋め込みホストデータの候補を最終的な埋め込みホストデータ W として選択する (S40)。埋め込み強度 S_i が基準値 T 以下の場合 (S30 の N)、現在の変数 i の値が L に等しいなら (S34 の Y)、これまで調べた埋め込み強度 S_k の値が最大となる添え字 k を変数 K に代入し (S38)、 K 番目の埋め込みホストデータの候補を最終的な埋め込みホストデータ W として選択する (S40)。現在の変数 i の値が L より小さいなら (S34 の N)、変数 i を 1 だけインクリメントして (S36)、ステップ S22 に戻る。

【0069】この繰り返し処理により、埋め込み強度が所望の基準値以上である候補が得られた時点で、その候補を最終的な埋め込みホストデータ W として選択し、そのような候補が生成されなければ、 L 個の埋め込みホストデータの候補を生成して、その中から埋め込み強度が最大であるものを最終的な埋め込みホストデータ W として選択することができる。

【0070】実施の形態 2

$$K = \arg \max_k \left(P_k / (2 \sigma_k^2) \right) \\ P_k = \sum_{i=0}^{n-1} \left| \sum_{j=0}^{m-1} (w^{*+k}_{i,j} - w^{*-k}_{i,j}) \right|^2 / n \\ \sigma_k^2 = \sum_{i=0}^{n-1} \left| \sum_{j=0}^{m-1} (w^{*+k}_{i,j} - w^{*-k}_{i,j}) - P_k^{1/2} \cdot x^k_i \right|^2 / n$$

ここで $w^{*+k}_{i,j}$ 、 $w^{*-k}_{i,j}$ は特定の処理がなされた後の埋め込みホストデータ W である。特定の処理がたとえば JPEG 圧縮であると分かっている場合、※

$$w^{*+k}_{i,j} = \text{round} (w^{+k}_{i,j} / q_{i,j}) \cdot q_{i,j} \\ w^{*-k}_{i,j} = \text{round} (w^{-k}_{i,j} / q_{i,j}) \cdot q_{i,j}$$

ここで $q_{i,j}$ は位置 (i, j) における JPEG の量子化テーブルの値である。round は JPEG 圧縮時に用いられる四捨五入の演算を行う関数である。

【0074】本実施の形態によれば、透かしの埋め込み時に、埋め込み後のホストデータに対する特定の処理を想定して埋め込み強度を評価し、埋め込み強度の高い透かしデータのビット系列を選択するため、特定の処理に対する耐性の強い電子透かし埋め込みデータを生成することができる。

【0075】実施の形態 3

図 12 は、実施の形態 3 に係る符号化装置 50 の構成を示す。この符号化装置 50 は、透かしデータ X をホストデータ V の複数の埋め込み位置の候補に埋め込み、透かしの耐性が強くなる候補を選択して、最終的な埋め込みホストデータ W として出力する。実施の形態 1 と共通する構成については同一符号を付して説明を省き、実施の

* 図 10 は実施の形態 2 に係る符号化装置 11 の構成を示す。本実施の形態では、電子透かしの埋め込まれたホストデータ V が受ける圧縮符号化などの特定の処理をあらかじめ想定し、透かしの埋め込み時にその特定の処理による影響を考慮して、電子透かしに耐性をもたせる。実施の形態 1 と共通する構成については同一符号を付して説明を省き、実施の形態 1 とは異なる構成と動作について説明する。

【0071】変更部 15 は、透かしデータ X をスクランブルする際、ホストデータ V が受ける特定の処理による歪み D を考慮して耐性の強い透かしデータのビット系列を選択し、スクランブルされた透かしデータ X' を出力する。図 11 は変更部 15 と埋め込み部 16 の機能構成図である。重みつき SNR 計算部 29 は、 L 種類のスクランブルされた透かしデータ X' が埋め込まれたホストデータ W の候補について、透かしデータ X の耐性を評価する際に、特定の処理により想定される歪み D を考慮に入れる。具体的には、埋め込まれた透かしデータと検出される透かしデータとの間の分散により埋め込み強度を評価する際に、埋め込みホストデータ W に対する特定の処理による劣化を考慮した以下の重み付け分散を用いる。

【0072】

※ $w^{*+k}_{i,j}$ 、 $w^{*-k}_{i,j}$ は JPEG の量子化テーブルを用いて次式により計算することができる。

【0073】

$$w^{*+k}_{i,j} = \text{round} (w^{+k}_{i,j} / q_{i,j}) \cdot q_{i,j} \\ w^{*-k}_{i,j} = \text{round} (w^{-k}_{i,j} / q_{i,j}) \cdot q_{i,j}$$

形態 1 とは異なる構成と動作について説明する。

【0076】位置検出部 52 は、スクランブルされた埋め込み位置 P を生成し、埋め込み部 54 は、秘密鍵 K を用いて、ホストデータ V の埋め込み位置 P に透かしデータ X を埋め込み、埋め込みホストデータ W を出力する。位置検出部 52 と埋め込み部 54 は協同して、複数の埋め込み位置 P を生成し、それぞれの埋め込み位置 P に透かしデータ X を埋め込み、複数の埋め込みホストデータ W の候補を生成し、それらの候補の一つを選択する機能をもつ。

【0077】図 13 は位置検出部 52 と埋め込み部 54 の機能構成図である。ECC 部 24 は透かしデータ X に誤り訂正のためのパリティを付加した透かしデータ X_e を生成する。位置情報生成部 60 は、ホストデータ V について L 個の埋め込み位置 P の候補を生成する。埋め込み部 26 は L 個の埋め込み位置 P の候補のそれぞれに

透かしデータX。を埋め込み、L種類の埋め込みホストデータWの候補を生成する。

【0078】位置情報生成部60は、GS方式によりL個のスクランブルされた埋め込み位置Pの候補を生成する。初期埋め込み位置 P^* に対して、L種類の初期データ $C_0 \sim C_{L-1}$ を与えて、実施の形態1に述べた方法により、初期埋め込み位置 P^* をスクランブルする。

【0079】図14は、実施の形態3に係る復号装置の構成を示す。この復号装置は、埋め込みホスト信号W'から埋め込まれた透かしデータX。を抽出し、この透かしデータX。に対して誤り復号し、誤り訂正がなされた透かしデータX。を得る処理を行う。位置情報生成部60は、図13に示した符号化装置50における位置情報生成部60と同様に、L個の埋め込み位置Pの候補を生成する。L個の抽出部42は、位置情報生成部60により与えられたL個の埋め込み位置Pの候補から、埋め込みホスト信号W'に埋め込まれたL種類の透かしデータX。の候補を抽出する。L個の埋め込み位置Pの候補の内、一つの候補が正しい埋め込み位置である。整合フィルタ62は、L種類の透かしデータX。の候補と、想定される透かしデータYとの間で相関を計算し、マッチングをとる。セレクト64が相関の最も高い透かしデータX。の候補を選択することで、正しい埋め込み位置にある透かしデータX。が得られる。さらに透かしデータX。は、ECC復号部44により誤り訂正がなされる。

【0080】想定される透かしデータYは、ホストデータVに埋め込まれた透かしデータXがあらかじめわかっている場合に与えられる。たとえば、ホストデータVの作成者があらかじめわかっており、その作成者の透かしデータXがホストデータVに埋め込まれているかどうかを確認する場合がある。一般に、本実施の形態は、埋め込まれている電子透かし情報があらかじめ想定されているが、透かしデータの埋め込み位置が候補としてしか与えられていない場合に適用することができる。

【0081】本実施の形態によれば、電子透かしを埋め込む対象となるメディアデータが与えられると、そのメディアデータに応じて、透かしデータを埋め込み易い位置を検出して、透かしデータを埋め込むことができ、埋め込まれる透かしの耐性を強化することができる。

【0082】実施の形態4

実施の形態1から3において、透かしデータXの誤り訂正のためにECCが用いられた。復号側で透かしビット x^k を検出する際、判定値 z_i が利用されていた点を考慮すると、透かしデータの検出には、ビットの値の確からしさを示す補助情報を復号判定に用いる軟判定復号が有効であることが理解される。本実施の形態では、そのような軟判定復号法としてターボ符号を用い、符号化側のECC部24、復号側のECC復号部44の代わりに、それぞれ図15のターボ符号化部70、図16のターボ復号部90を用いる。

【0083】図15を参照してターボ符号化部70の構成と動作を説明する。符号化の対象として入力されるユーザビット列UBは、第1符号化器72に入力され、パリティビット列P。が生成される。ユーザビット列UBはインターリーバ74により順序が並べ替えられて、第2符号化器76に入力され、パリティビット列P₁が生成される。2つのパリティビット列P。、P₁はマルチプレクサ・パンクチャ78により、間引き(puncture)されながら多重化され、さらにユーザビット列UBと多重化されて符号化ビットCBとして出力される。なお、パンクチャの処理は、埋め込みビット数を増加させたいときに用いられるオプションな処理であり、必要でない場合は省略してもよい。

【0084】図16を参照してターボ復号部90の構成と動作を説明する。図15の第1符号化器72に対応する第1軟復号器92は、受信したチャネル出力COを復号し、各情報シンボルの復号結果とそれに対する信頼度の情報を与える外部情報(Extrinsic Information)を出力する。ここで、受信したホストデータから判定値として抽出される軟値 z_i がチャネル出力COとして扱われる。図15の第2符号化器76に対応する第2軟復号器98は、第1軟復号器92からインターリーバ94を介して得た外部情報を事前確率として用いて、インターリーバ96により順序を並べ替えられたチャネル出力COの復号処理を行い、復号結果に対する外部情報をデインターリーバ100を介して第1軟復号器92に与える。第1軟復号器92は第2軟復号器98からの外部情報を事前確率として用いて、チャネル出力COの復号処理を行う。この一連の動作を繰り返し行うことで、ターボ復号部90は最終判定FDを出力する。インターリーバ94、96による並べ替えは、図15のインターリーバ74の並べ替えと同じである。またデインターリーバ100はインターリーバ94、96の並べ替えを元に戻す処理を行う。

【0085】ターボ復号部90では、第1符号化器72と第2符号化器76が、互いに他方から提供される事前情報を利用し合って、MAP(Maximum A posteriori Probability)復号による復号結果を逐次的に改善することができる。これにより透かしビットを検出する際のビット誤り率(BER)をさらに低減することができる。

【0086】以上、本発明を実施の形態をもとに説明した。これらの実施の形態は例示であり、それらの各構成要素や各処理プロセスの組み合わせにいろいろな変形例が可能で、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0087】そのような変形例として、実施の形態2における特定の処理を想定して埋め込み強度を評価する方法は、実施の形態3における埋め込み強度の評価の際にも適用することができる。

【0088】複数の透かしデータの候補または埋め込み

位置の候補を生成するために、多様性に富んだ候補の生成が可能なGS方式を用いたが、他のスクランブル方式を適用してもよく、また何らかの方法でランダムに候補のデータを生成してもよい。また実施の形態では、逆スクランブルにより、生成された透かしデータの候補から元の透かしデータを再現したが、生成された透かしデータの候補と元の透かしデータとを対応づけたテーブルを備え、このテーブルを参照して元の透かしデータを求め

てもよい。
【0089】またスクランブルの際に初期データとして使用した識別データは、透かしデータの先頭に挿入されて復号側に提供されていたが、この識別データを透かしには埋め込まずに、符号化側で秘密鍵として保持、管理してもよい。その場合、復号側はこの秘密鍵を取得した上で、透かしデータのスクランブルを解除する。また実施の形態3では、復号側でこの識別データを秘密鍵として入手する場合は、埋め込み位置が秘密鍵から特定されるため、整合フィルタ62による埋め込み位置の検出作業が不要となり、したがってあらかじめ想定される透かしビットを用意しておく必要もなくなる。

【0090】また実施の形態4ではターボ符号を説明したが、軟判定の可能な誤り訂正符号であれば他の符号化方法を用いてもよい。

【0091】なお、実施の形態1の変形として、逐次型の候補の生成、評価のための構成と動作を説明したが、同様の逐次型の構成と動作が、実施の形態2および3にも適用できることはいうまでもない。

【0092】実施の形態3では、埋め込み位置の候補をスクランブル方式により生成したが、埋め込み位置の候補を次に述べるテーブルマッチングによりランダムに生成してもよい。このために、電子透かしの埋め込み側と抽出側は、埋め込み位置の候補を識別するための識別データと埋め込み位置とを対応づけたテーブルを備える。このテーブルは、透かしデータの第1ビットについて、たとえば、「識別番号0の場合は(1, 29)の位置、識別番号1の場合は(983, 251)の位置、・・・、識別番号15の場合は(542, 37)の位置に埋め込む」といった識別番号と埋め込み座標との対応関係を格納する。第2番目から第n番目のビットについてもそれぞれ埋め込み位置が異なる対応関係が格納される。埋め込み位置は何らかの方法でランダムに生成される。埋め込み側では、このテーブルを参照して、埋め込み位置の候補の識別データに対応づけて埋め込み位置の候補を生成し、透かしデータをその候補の位置に埋め込む。抽出側では、埋め込み位置の候補の識別データにもとづいてこのテーブルを参照することにより、埋め込み位置を特定し、透かしデータをその位置から抽出する。この方法によれば、埋め込み位置のランダム性が十分に保証され、頑強な埋め込みを実現することができる。また抽

出側では、埋め込み位置の候補の識別データ以外にこのテーブルをもっていなければ、埋め込み位置を知ることができないため、セキュリティを高めることができる。

【発明の効果】本発明によれば、電子透かしの耐性が向上し、透かしの検出精度が改善する。

【図面の簡単な説明】

【図1】 実施の形態1に係る符号化装置の構成図である。

【図2】 図1の変更部と埋め込み部の機能構成図である。

【図3】 実施の形態1に係る復号装置の構成図である。

【図4】 元の透かしデータとL種類のスクランブルされた透かしデータとの関係を説明する図である。

【図5】 符号化時の畳み込み演算を説明する図である。

【図6】 復号時の畳み込み演算を説明する図である。

【図7】 図7(a)、(b)は、スクランブルされた透かしデータの埋め込み方法を説明する図である。

【図8】 符号化装置による電子透かしの埋め込み手順を説明するフローチャートである。

【図9】 符号化装置による別の電子透かしの埋め込み手順を説明するフローチャートである。

【図10】 実施の形態2に係る符号化装置の構成図である。

【図11】 図10の変更部と埋め込み部の機能構成図である。

【図12】 実施の形態3に係る符号化装置の構成図である。

【図13】 図12の位置検出部と埋め込み部の機能構成図である。

【図14】 実施の形態3に係る復号装置の構成図である。

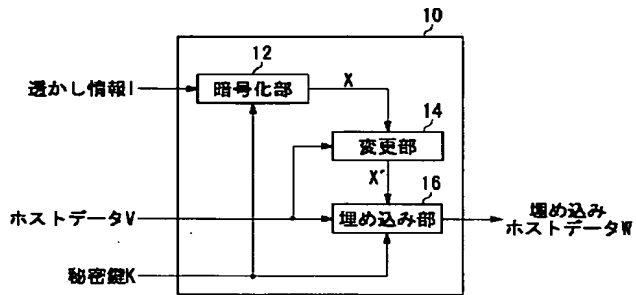
【図15】 実施の形態4に係る符号化装置のターボ符号化部の構成図である。

【図16】 実施の形態4に係る符号化装置のターボ復号部の構成図である。

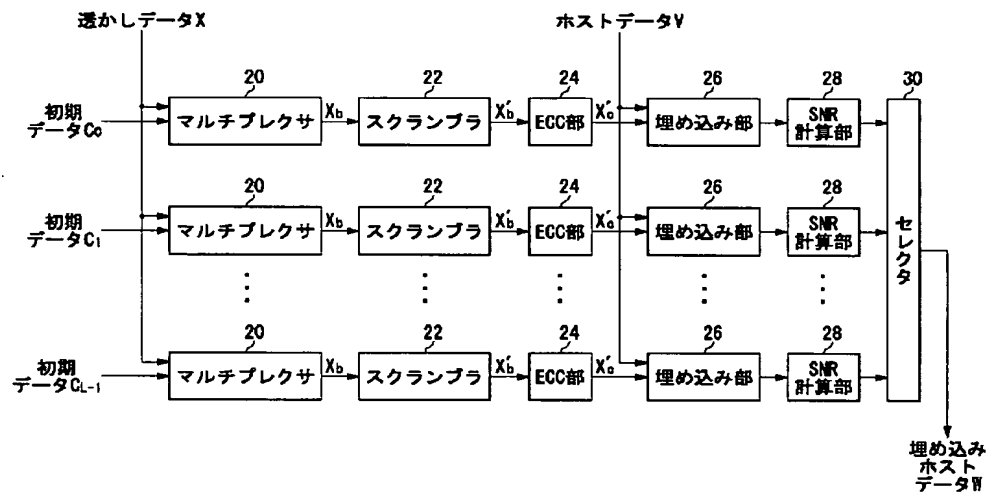
【符号の説明】

10 符号化装置、 12 暗号化部、 14 変更部、 16 埋め込み部、 20 マルチプレクサ、 22 スクランブラ、 24 ECC部、 26 埋め込み部、 28 SNR計算部、 29 重みつきSNR計算部、 30 セレクタ、 40 復号装置、 42 抽出部、 44 ECC復号部、 46 デスクランブラ、 50 符号化装置、 52 位置検出部、 54 埋め込み部、 60 位置情報生成部、 62 整合フィルタ、 64 セレクタ、 70 ターボ符号化部、 90 ターボ復号部。

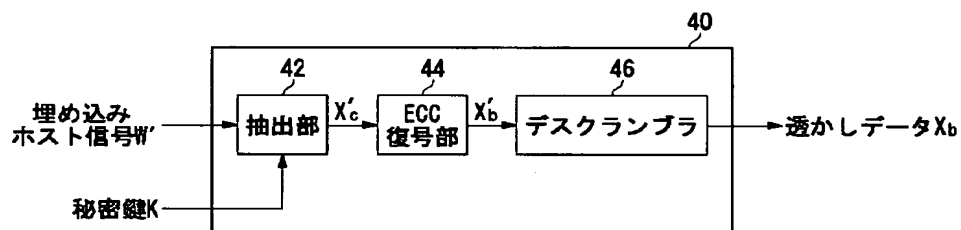
【図1】



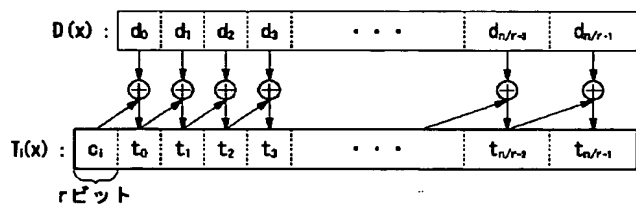
【図2】



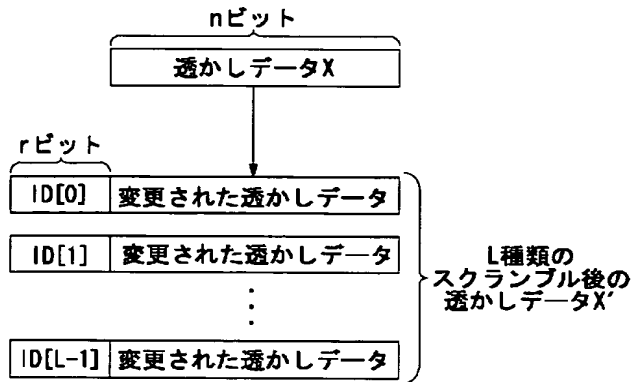
【図3】



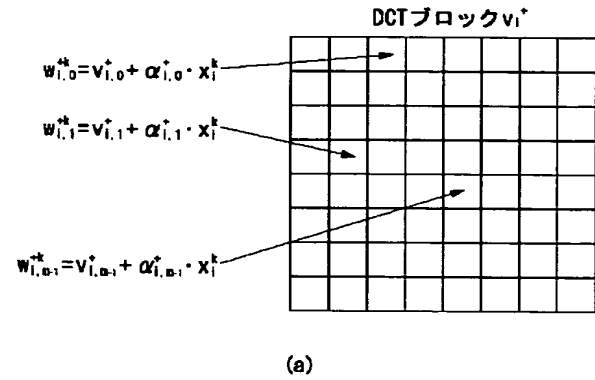
【図5】



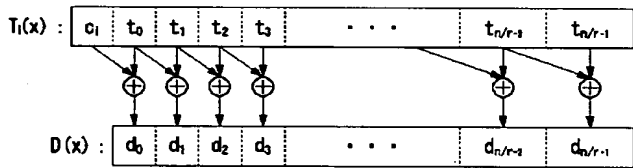
【図4】



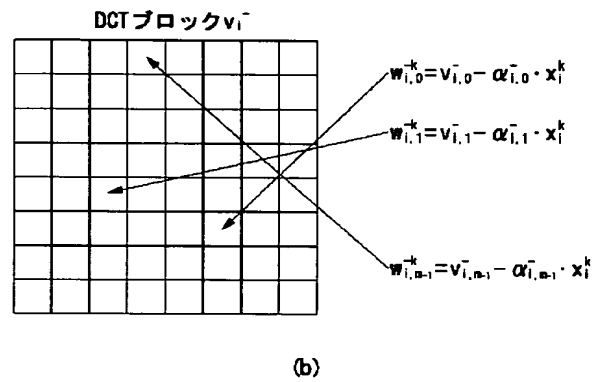
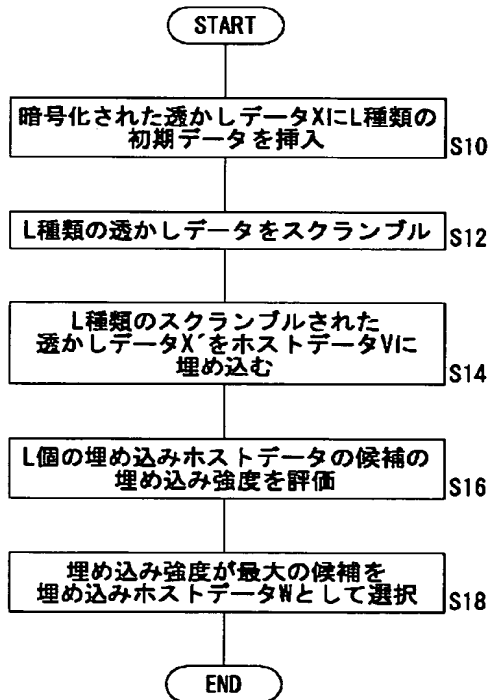
【図7】



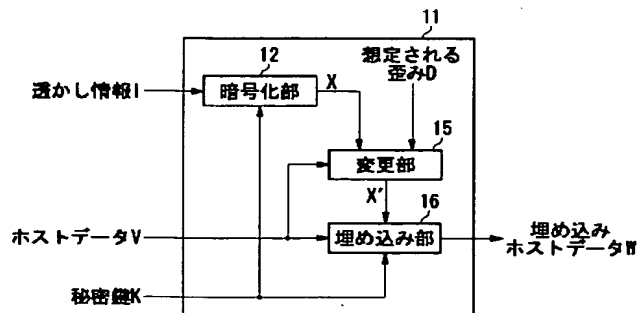
【図6】



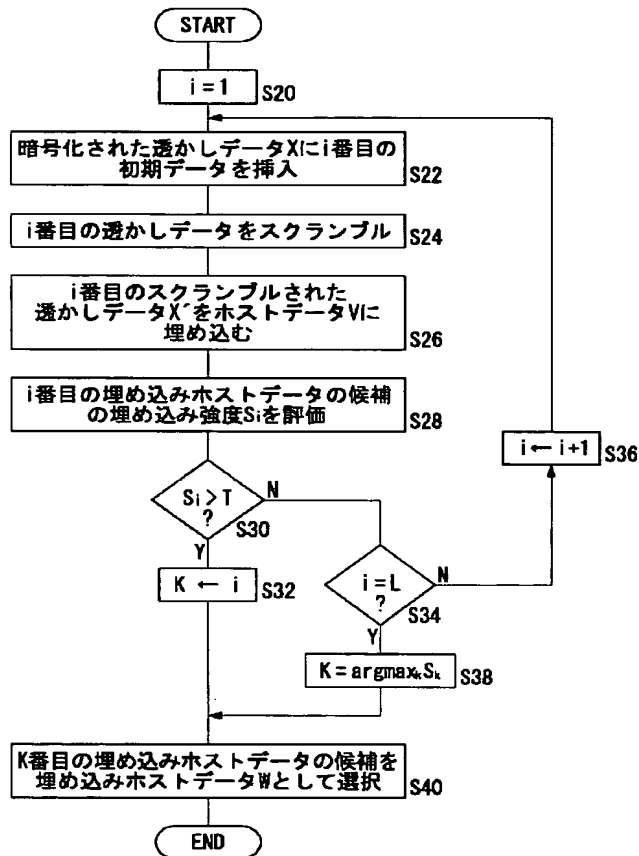
【図8】



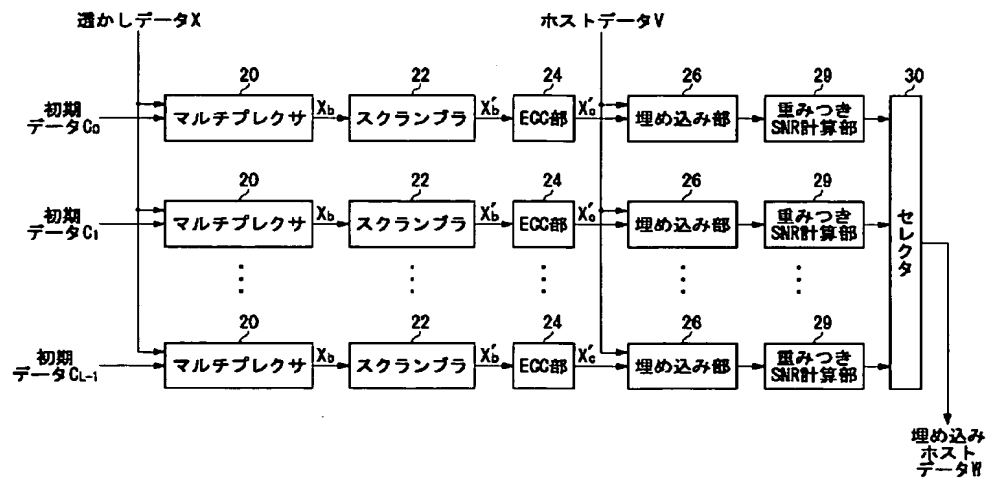
【図10】



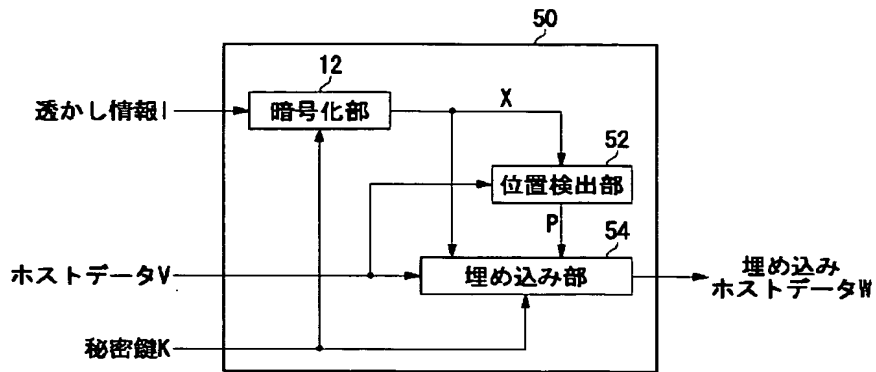
【図9】



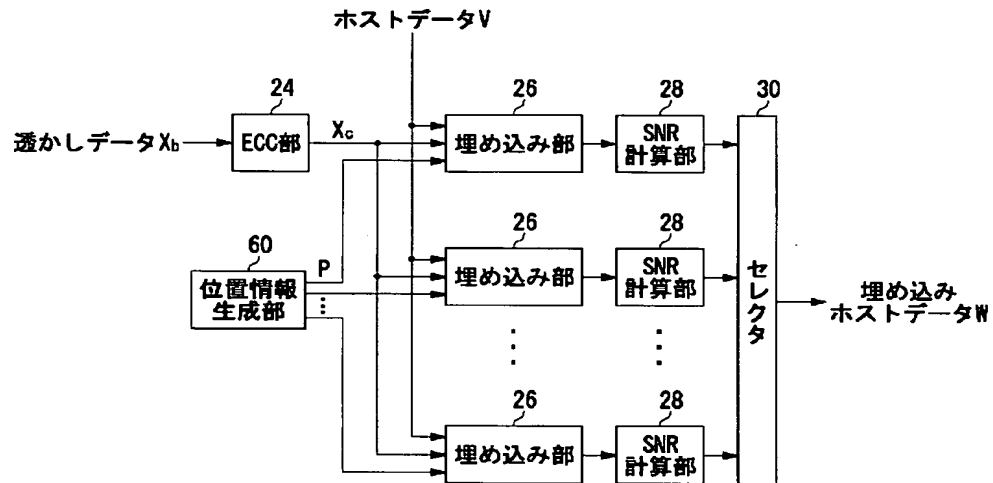
【図11】



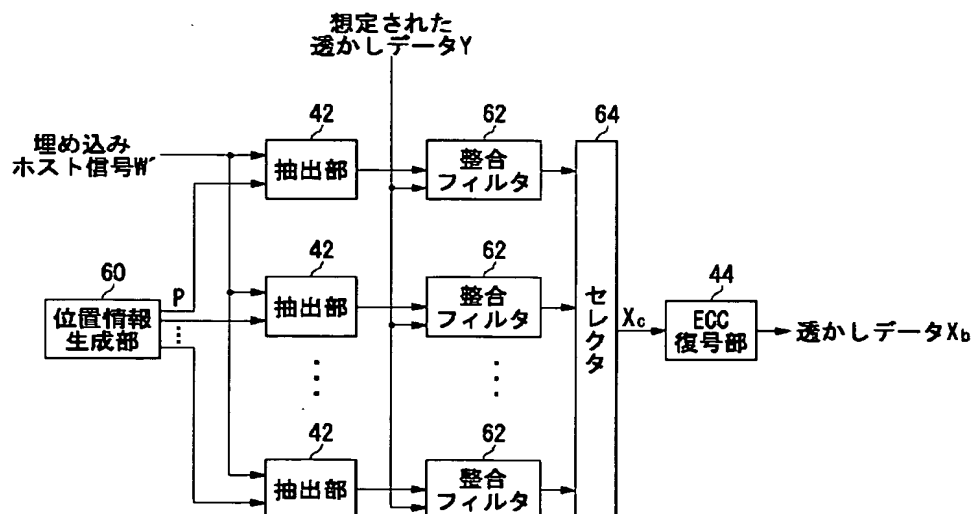
【図 12】



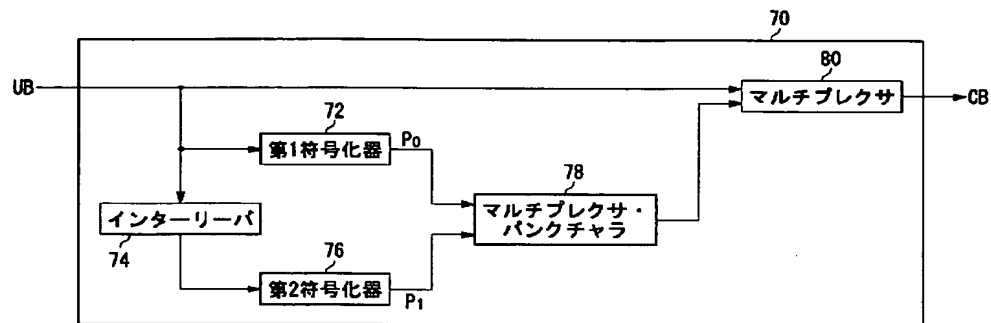
【図 13】



【図 14】



【図 15】



【図 16】

